SAP GRC Access Control 10

Frequently Asked Questions

v1.0 (26th Sep 2016) – 50 questions

by:

Raghu Boddu

GRC SME/Architect – Expert in Solution Tweaking

raghu@sapsecurityexpert.com

Question # 1 - How to archive obsolete data in GRC Access Control 10?

The data in the GRC AC such as Requests, EAM Audit logs, Change Logs, have to be archived for audit purpose. SAP GRC doesn't have an in-built archiving capabilities.

Below steps can be followed to archive the GRC AC 10x data:

Use Transaction SARA

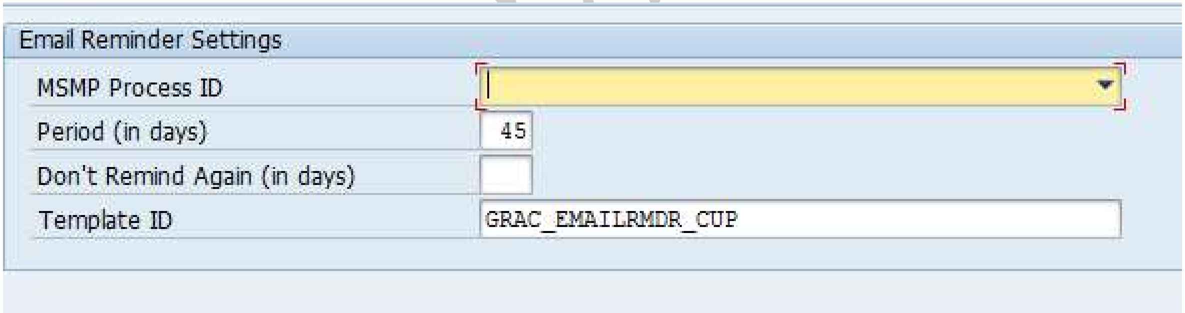
The following are objects to archive:

GRFNMSMP - Archiving for GRC AC requests
SPM_AU_LOG - EAM Audit Log Archive
SPM_CH_LOG - Change Log Archive (EAM)
SPM_OC_LOG - EAM OS Command Log Archiving
SPM_SY_LOG - SPM System Log Archive.

Refer SAP Note **1719967** - How to archive in GRC Access Control 10.0 for detailed steps.

Question # 2 – How to setup email reminder notifications in GRC AC 10x?

Use the program GRFNMW_BATCH_EMAIL_REMINDER for scheduling the email reminders. Parameters such as Process ID, period, Template can be selected while scheduling the job:



Email Reminder Settings

MSMP Process ID	
Period (in days)	45
Don't Remind Again (in days)	
Template ID	GRAC_EMAILRMDR_CUP

Question # 3 – How to clean-up the completed background jobs in GRC AC 10x?

Access Control applications do not have a feature to delete spools as this function is not approved by the auditors. The audit policies recommend for data retention. Instead, it is recommend to archive the spools.

Please consult with your BASIS or DBA team to determine the possible solution to automate the process of archiving these log files.

Question # 4 – How to optimize the GRC AC10 database?

In GRC AC, majority of the database utilization will be by the Access Risk Analysis. The Batch Risk Analysis will synchronize users, roles, and profiles data and keeps a snapshot for all the systems. This data is used for the GRC AC management reports and offline Risk Analysis.

Normally when the Batch Risk Analysis is schedule for the 1st time, the DB growth will be huge and the next time, it will be very less growth since it will analyse only the incremental objects (ex: only new or changed users from the last execution) and store the violations. This initial large DB growth depends on rule set, number of authorizations and number of violations per user, role, and profile which may be large if users/roles were never cleaned up.

To drastically reduce the DB size, it is recommend to set the AC configuration parameter 1027 (Enable offline Risk Analysis) to 'No'. Thiswill drastically reduce the database growth from batch risk analysis but still update the management dashboard data.

Please note that this option is not viable if you wanted to use the offline analysis instead of real time ad-hoc analysis or use the report SoD Review or wanted to enable the BI reporting.

Solution:

The quick option to reduce the DB size is to delete the Ad-hoc risk run results that are stored in the table following tables:

- GRACSODREPDATA
- GRACSODREPINDEX
- GRACSODREPSTATUS

These tables are populated with the ad-hoc risk analysis data every-time we run the risk analysis in the background or foreground mode, thus the table size will grow. The data is appended and not overwritten every time you run a risk analysis.

The growth of the data in these tables can be controlled by using the program **GRAC_DELETE_REPORT_SPOOL**. You may schedule this as a daily job or you can delete the data manually whenever you want.

If you still feel the data is huge you can change the storage location from database to file system using the parameter 1053 - Spool Type to File (By default it is Database).

Below programs are utilized to clean the rules:

- GRAC_DELETE_ACCESS_RULES (Connector can be selected.)
- GRAC_DELETE_ACCESS_RULES_ALL (deletes the rules for all the connectors)

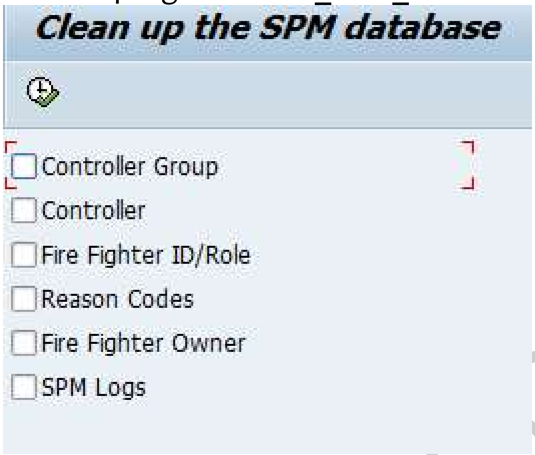
NOTE: Use the utility - **GRAC_EXPORT_REPORT_SPOOL** to export the data of a specific job.

Additional references:

1580877 - Best practices in storage management for SoD analysis jobs
1646988 - AC V10 Spool icon is not displaying next to ad hoc risk analysis background job ID
1700811 - Scheduling the action usage full sync job

Question # 5 - How to clean-upEAM (SPM) database?

Use the program GRAC_SPM_CLEANUP. This will clean-up following:



Clean up the SPM database

□ Controller Group
□ Controller
□ Fire Fighter ID/Role
□ Reason Codes
□ Fire Fighter Owner
□ SPM Logs

NOTE: It is not recommended to cleanup this data. Consult you your Internal control/audit/BCO team to know how to manage this data effectively.

Question # 6 - What are Work Centres, Work Sets, and Work Items?

Workcenters are the top menu items in the NWBC screen. Worksets are the group of the related items and Work items are the individual clickable links.

Question # 7 - Which add-on is required to install GRC AC?

GRCFND_A – GRC Foundation for ABAP. You can check the existence of this Add-on either from SAINT transaction code or from the System → Status, Components Version.

The Version of GRC 10 Add-on is V1000, and GRC 10.1 is V1100

Question # 8 - Can we install SAP GRC v10 on SAP 4.6c system?

No. GRCFND_A (GRC Foundation for ABAP) requires minimum a SAP NetWeaver ABAP AS 7.02 system. Since SAP 4.6c (Enjoy SAP) is not a NetWeaver product, it can't be installed on a SAP 4.6c. However, an SAP 4.6c system can be connected as a satellite (backend) system for provisioning purpose.

Question # 9 - How can I connect a HR system to GRC?

The **GRCPIERP** plugin has to be installed in the backend HR system. The plug-ins are available for download from the SAP market place. However, to utilize the complete functionality of HR triggers, additional configuration is required. You can refer the below link to understand the process of configuring "HR Triggers" in GRC:

https://wiki.scn.sap.com/wiki/display/GRC/Understanding+HR+Triggers+in+Access+Control+10.0

Question # 10 - What is MSMP & BRF+?

Answer source - http://sapinsider.wispubs.com/

MSMP is the new workflow engine used within GRC Access Controls 10.0. It stands for Multi-stage, multi-path meaning that the engine is capable of directing requests down multiple approval routes simultaneously. It is used for the management of automated approval workflows for the purposes of access request management but can also be triggered for the other access control modules including Access Risk Analysis master data updates or role build approval workflows. The big change is that it works off a multitude of different rules to govern what should happen to the requests. All of these rules need to be defined up front before they can be assigned in to the configuration and used in the workflow processes.

BRF+ is the Business Rules Framework Plus application which supports the definition of business rules. It can be the authoring environment for the rules which can then be plugged into MSMP workflow configuration. However, it is much more powerful than that. In advanced cases, it can actually be like writing code but for access controls functionality, the uses are often more simple to derive agents or specific results which can be linked to workflow route decision points.

The biggest change is definitely the terminology. The existing capabilities are still there within MSMP but they are called different things:

- There is still an initiator although this is now a central and global initiator for each workflow process (type). Rather than specifying an initiator for each workflow path, you now only have one which contains all of the different variations that you can have.

- Paths are still the same as are stages but Approvers are found through Agent Rules rather than CADs.
- Agent rules are also the source for defining recipients of notifications.
- Further changes are to be found in the architectural changes. Being on ABAP, the solution now requires more SAP standard setup. For example, you have to activate the tasks for SAP business workflow and configure SAPConnect to be able to send email notifications.
- Also, the content is transportable to enable you to migrate through the landscape. This also requires attention as although the configuration is transported, you'll still need to check the master data (user IDs) and activate the workflow locally in each system.

Question # 11 - What is the advantage of installing BI Content and connecting BI system to GRC system?

When you install BI content, all the GRC related InfoCubes, InfoObjects will be created in the BI system along with some default reports. This will help you to create custom reports as per the management requirements.

Question # 12 - what are the post installations steps in the GRC system?

1. Activating the Applications(SPRO → IMG → GRC → General Settings)** TR is required.
2. Activating the ICF services using tcode SICF (you need to at least activate PUBLIC, GRC, BC SETS services)
3. Ensure that ICM services are also configured using SMICM (Goto transaction code SMICM→ Goto → Services and ensure that your HTTP and SMTP services are enabled).
4. Activate BC sets Tcode is **SCPR20**
5. Maintain system parameters

Question # 13 - What is the best recommended landscape for SAP GRC?

This is a quite common question which is coming up a lot during the early scoping phases of projects and also on the training courses I've taught. It is important to understand what you want to do with your GRC system and then look at how best to architect it.

I think GRC has a massive role to play in supporting both production and non-production systems from the perspective of controls and efficiency. However, it can create massive complexity in your connector configuration to support that and actually open up a different set of risks. The main advantages of connecting GRC prod to SAP pre-prod is in Role build as you can then track all of the compliant role build processes throughout the landscape.

You can do risk analysis against a productive ruleset from anywhere in your SAP landscape. You can also check for critical development access (developer and transport activities) from your

GRC production system. It is also much more efficient to have a single user management workflow process for all systems.

It gets complicated when you factor in the GRC pre-production environments. You need to validate your GRC changes against a system somewhere and you need to be clear which system is the one you want to rely on and which is supporting testing. For eg: you could actually provision access from GRC dev for unit testing, GRC QA for UAT and from GRC prod for actual users which actually then complicates the risk of user provisioning standards massively.

Question # 14 - What are the steps to create CONNECTOR?

To connect a new ABAP client/connector, you should have the RFC connections (in both the systems) ready. Follow the below steps to add a new connector to GRC system:

1. Maintain CONNECTOR Settings (SPRO → IMG → GRC →Common Component Settings→Integration Framework)
2. Define the connection type as SAP using "Maintain CONNECTION type" option
3. Maintain Logical CONNECTOR groups.
4. Add the CONNECTOR to the CONNECTOR groups.
5. Maintain CONNECTION settings
6. Maintain CONNECTOR settings

Once the connector is added, run the Authorization Sync and the Repository Object Sync job.

Question # 15 – Define the terms ARA, Risk, Action and Permission?

ARA stands for Access Risk Analysis, a component of SAP GRC to identify the Critical Risk & Segregation of Duties. It allows to effectively manage the risks by adapting the right remediation approach for the risks.

A "transaction code" is referred as "**Action**" and an "Authorization object" is referred as Permission in the GRC terminology.

Risk - A probability or threat of damage, injury, liability, loss, or any other negative occurrence that is caused by external or internal vulnerabilities, and that may be avoided through pre-emptive action.

In business terms, Risk is the probability that an actual return on an investment will be lower than the expected return.

Question # 16 - What are the different type of risk?

In SAP GRC, you can identify the following types of risks:

1. Critical Action (Critical Transaction code)
2. Critical Permission (Critical Authorization Object)
3. SOD Risk (Conflict at the transaction code or the authorization object level)
    a. Action level
    b. Permission level

Risks can be identified using the ARA (Access Risk Analysis) component of SAP GRC.

Question # 17 - What is a Ruleset?

Ruleset in GRC is the collection of rules (standard or customised) which prevent the potential risks to the business in terms of transactions by user. Technically, Ruleset is a combination of Risks, Function and Business Process.

Once the Ruleset related BC Sets are activated, Rules must be generated. This can be done in SPRO (GRC > Access Control > Access Risk Analysis > SOD Rules > Generate SoD Rules).

SAP delivers the default ruleset called as "**Global Ruleset**".

Question # 18 - What are the prerequisites for using MSMP workflows?

The Workflows should be activated and there is a pre-defined configuration that needs to be completed before using the workflows. Below document explains you the detailed steps of setting up workflows:

http://www.sdn.sap.com/irj/scn/go/portal/prtroot/docs/library/uuid/80088ef0-2590-2e10-7696-fa36bfcff700?overridelayout=true

NOTE: ARM is mandatory for Workflows. Incase if you are only configuring EAM, and ARA ensure to maintain the "Integration Scenario" for all the 4 components.

Question # 19: What are the various modes of Risk analysis?

Online Risk: Online Risk Analysis is also termed as "Real-time Analysis" or "Adhoc Analysis'. In an Online Risk Analysis, GRC system will read the user data (role assignment data) from back-end system every time when the risk analysis is executed.

Offline Risk: The Risk Analysis will be performed with the user data and role data that is available within the GRC repository box. Offline Risk Analysis is mostly performed for doing a Mass Risk Analysis. It is always recommended to run the GRAC_REPOSITORY_OBJECT_SYNC job before performing an offline Risk Analysis.

Question # 20: Why Ruleset needs Customization?

The SoD rule set should be customized for your specific business. The default ruleset (Global) is too broad to cover multiple scenarios and industries. Since, organizations configure SAP differently to support their unique business processes, the default ruleset may not be applicable AS IS to your organization.

Thus, it is important to customize the risks to reflect the magnitude of relevant risks and make them fit for your organization requirements. Customizing will ensure accurate reporting

Further, the default ruleset does not include any custom transactions. You can accommodate the risks from the custom transactions.

Question # 21: What are the different types of Risk Analysis? How to perform Risk Analysis?

Risk Analysis can be performed at:

User Level (Referred as Extra level Risk Analysis) - Displays the risks that occur due to assigning of multiple roles. .

Role Level (Referred as Intra Level Risk Analysis) – Displays the risks that occur due to various conflcting and critical transaction codes within the same role.

HR Objects Level – Identifies the risks at the Organization Unit, Job, and Position level.

Profile Level – Identifies the risks within the profile.

To run the Risk analysis, go to NWBC→ Access Management Work Center → Select the relevant Risk Analysis type (User, Role, HR object, Profile Level)

NOTE: Simulation options can be used to simulate a transaction code/role assignment before it is actually assigned.

Question # 22: What is the difference between Intra Level Conflicts and Extra Level Conflicts?

Intra Level Conflicts: The Risk that exits in the same role is referred as Intra Level Risks/Conflicts. It is always recommended to identify and address the risks at the role level before addressing at the user level.

Extra Level Conflicts: These are the conflicts that occur due to combination of roles. When roles are assigned to a composite role, or a user, it is recommended to perform the Risk analysis and identify the extra level conflicts.

Question # 23: what is a Mitigation Control?

Mitigation Control is often called as Compensating Control or a "Internal Control" Document. It is required that the selected SOD conflicts be addressed properly. Incase, if segregation of duties cannot be achieved due to a lack of personnel or other reasons, compensating controls (mitigating controls) need to be implemented to minimize the risks of accumulation of duties.

The following lists the various types of compensating controls that management should consider implementing when there is inadequate segregation of incompatible duties:

- **Second signature**: Two signatures/approvals required to authorize bank payments, salary transfer initiation, purchase orders, etc.
- **Review by a supervisor**: The daily journal entries report reviewed and signed by the supervisor of the person responsible for posting the journal entries
- **Exception reports**: These reports should be reviewed in a timely manner, checked against supporting documents evidencing authorization and signed by supervisor. Some examples of reports (preferably SAP standard reports and system-generated):
- **Report of changes performed to G/L accounts** -> report of updated/opened GL accounts
- **Report of postings recorded on accruals accounts**
- **Report on pending items resulting from reconciliations** (e.g. bank reconciliation, G/L and sub-ledgers reconciliations, etc)
- **List of adjustments** to a prior period
- **Report of payments above a given threshold**
- **Report of changes** performed on customer master data etc.,

For example, when a user can perform all the key activities of a transaction without adequate segregation of duties, an independent review of the detailed transactions for the department has to be performed on a regular basis to identify, investigate and correct improper/erroneous transactions. This must definitely be done by a second, independent person.

Furthermore, it is highly recommended that compensating controls are reviewed and checked for evidence (e.g. if reports have been reviewed) periodically by an independent person (e.g. internal audit) to ensure that alternative controls are working accordingly.

Question # 24: What are the pre-requisites to create a Mitigation Control?

To create a mitigating control, you need:

- The root Organization has to be created. (It require atleast one Organization unit)
- A Mitigation Control Owner.
- A Mitigation Control Monitor.
- Atleast one Risk ID.

Also, ensure that:

1. You have a defined rulebook.
2. You have updated all risks for the specific connector groups and generated the rules.
3. You have run risk analysis in your system.

Question # 25: what are the steps to create a Mitigation Control?

Before creating a mitigating control, ensure to create a Root Org entry (this replaces the Business Units in previous AC versions). To create a new root org entry, navigate to the IMG under Shared Master Data Settings and create a Root Org.

Additionally, you need atleast 1 Mitigating Control Owner, and 1 Mitigating Monitor. Once you assign the relevant authorization to the users, perform the following to create a mitigating control:

Goto NWBC > Setup > Mitigation Controls > Create

If the Workflow is enabled, the mitigating control will be created only upon approval of the Owner and the other approvers (as per the workflow definition). To check if the Mitigating Control workflow is enabled, check the parameter 1061. (If this is set to Yes, then the workflow will be triggered).

Question # 26: How to Mitigate the Risk? What is the Mitigation Process?

They are three ways to mitigate the Risk:

a. From the **Risk Analysis** Screen →Select the Risk click on "Mitigate Risk" button, select the right mitigating control and click Save/Submit.
b. NWBC→Access Management Work Centre → Mitigated Access Work Set group → Mitigated User Option. (This will allow to mitigate multiple users for a respective mitigating control)
c. Using the ABAP reports "**GRAC_DOWNLOAD_MIT_ASSIGNMENTS**" (To download the existing mitigation data) and "**GRAC_UPLOAD_MIT_ASSIGNMENTS**" (To upload the mass mitigations for multiple mitigating controls)

Question # 27: What is Critical Action Risk? How to create it?

Critical Action Risks are the critical transaction code risks. These risks doesn't require to be conflicted with other transaction code. Below are the steps to create a Critical Action Risk:

1. From NWBC > Setup Work Center, create a new function
2. Click Function work item and enter all the details (NOTE: Function can have multiple tcodes too)
3. From NWBC > Setup Work Center, create a Risk.
4. Add the newly created Function, Assign to atleast 1 Ruleset and assign a Risk Owner.
5. Select the newly created risk and "Generate Rules".

Question # 28: what is a Rule Generation? What are the different ways to generate rules?

When a new risk is created/modified, rules should be re-generated again to populate the corresponding Rulesets with the newly created risk(s) information. Rule generation will assign unique rule ID to every rule which is generated logically.

Following are the different ways to generate Rules:

1. NWBC > Setup > Functions > Select All (or respective function) > click "Generate Rules"
2. NWBC > Setup > Access Risks > Select All (or respective function) > click "Generate Rules"
3. SPRO > IMG > GRC > AC > Access Risk Analysis > SoD Rules > Generate SoD Rules

Question # 29: How many functions can have a Critical Action/Permission Level Risk can have?

Critical Action/Permission Risk can have only one function. Each function can have any number of Transaction codes/authorizations.

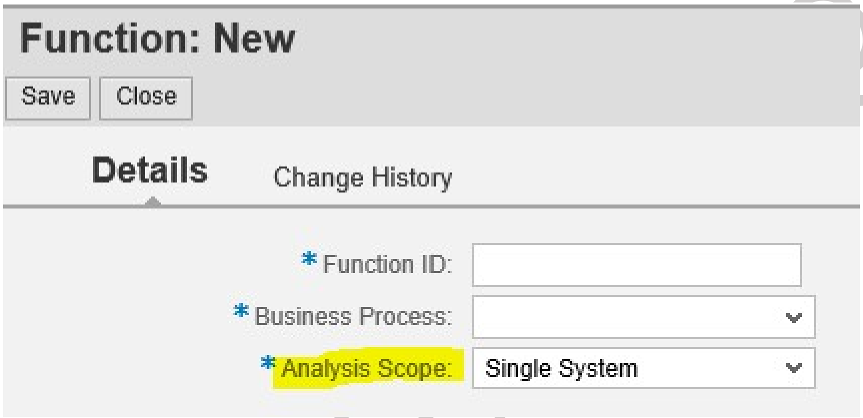
Question # 30: How to a cross system risk? How to create it?

Cross system risks are the risks that are occurred due to conflicting authorizations in two different systems. Below is an example:

- Creation and Maintenance of Purchasing Documents (PR, PO, Contracts etc.,) is done in SRM.
- Goods Receipt and Invoice Processing related activities are carried out in MM and FI-AP (In the ECC system)

If any user has authorization to perform both the activities, it is considered as a risk. However, this risk is not occurred in a single system, and is classified as a cross system risk.

Cross system risks have to be defined while creating a new function. Select the "Analysis Scope" as "Cross system"


Function: New

Save | Close

Details | Change History

* Function ID:

* Business Process:

* Analysis Scope: Single System

Question # 31: What is a Critical Permission Risk?

A Critical Permission is created to define an authorization object as Critical. GRC Access Risk Analysis allows to define risks at 4 levels 1) Roles 2) Profiles 3) Transaction codes 4) Authorization Objects.

Authorization objects such as S_DEVELOP, S_ALV_LAYO, S_ADMI_FCD etc., are classified as critical authorization objects and possess a risk even when they are assigned through a display or reporting transaction codes.

Critical Permissions risks can be created from NWBC > Setup > Risks.

Question # 32: What is the use of Detour/Routing path?

Detour (referred as Routing Rule in GRC 10) rule is a condition based rule which triggers a value based on satisfaction of a condition. But these standard rules are inflexible, so if you want to add another condition for routing along with risk violation or any different condition then you will have to change the ABAP logic within these function modules.

Instead, you can use the BRF+ functions to add a condition based logic.

Question # 33: What is Batch Risk Analysis? How to run Batch Risk Analysis?

The risk analysis in Reports and Analytics tab is always offline analysis and hence you should have run the "Batch risk analysis" to populate the violations data accurately.

Batch risk analysis can be performed in 2 modes:

1. Full sync mode
2. Incremental mode

Full sync mode will synchronize complete roles, profiles, and users. It is advised to run the Batch risk analysis in Full sync mode atleast once in month so that the Risk Analysis reporting will be more accurate. Below parameters are recommended:

1120	Batch size for Batch Risk Analysis
1121	Batch size for User sync
1122	Batch size for Role sync
1123	Batch size for Profile sync

However, the incremental mode is scheduled once in a day (normally after the PFCG_TIME_DEPENDENCY job).

Batch Risk Analysis can be setup via t-code GRAC_BATCH_RA.

Question # 34: How will you control GRC system if you have multiple rulesets activated?

SAP Access Control 10.0 provides users the flexibility to create and maintain multiple rulesets. A typical organization needs to manage multiple rulesets for various reasons ranging from business process control structure to organizational structure make-up. SAP Access Control allows you to choose from more than one ruleset to perform risk analysis automatically. This capability is also seamlessly supported in access request management functionality.

More important, you can build Business Rule Framework plus (BRF plus) logic to default a specific ruleset to an access request once defined criteria are satisfied. This is essentially the business case on which I focus. This is a way to eliminate the need for a manual field (ruleset) update and also to enforce control so that the risk analysis is executed using the correct and appropriate ruleset, thereby making the entire process of risk analysis less error prone.

Question # 35: What are the various background jobs for SAP GRC. How frequently they have to be scheduled??

Below are the important list of jobs that needs to be scheduled:

Job	Frequency	Description
GRAC_ACTION_USAGE_SYNC	Daily	Action Usage Job
GRAC_PFCG_AUTHORIZATION_SYNC	Weekly	Profile Generator (PFCG) roles authorization
GRAC_ROLE_USAGE_SYNC	Daily	Role usage synchronization
GRAC_ROLEREP_PROFILE_SYNC	Daily	Role repository profile synchronization
GRAC_ROLEREP_ROLE_SYNC	Daily	Role repository role synchronization
GRAC_ROLEREP_USER_SYNC	Daily	Role repository user synchronization
GRAC_SPM_AUDIT_LOG_SYNC	Weekly	Emergency Access Management (EAM) audit log synchronization
GRAC_SPM_LOG_SYNC_UPDATE	Weekly	Emergency Access Management (EAM) log synchronization
GRAC_SPM_WORKFLOW_SYNC	Weekly	Emergency Access Management (EAM) workflow synchronization
Batch Risk Analysis	Daily	Risk Analysis Job

NOTE: It is highly recommended to schedule the jobs to run at separate times. Also, be sure the database is sized sufficiently.

Run the jobs for one connector at a time, create variants to run the jobs, use incremental when possible.

Question # 36: How to download, upload and transport a Ruleset?

The SAP GRC ruleset can be downloaded, and uploaded using the newly added programs in GRC 10. A common problem for SAP Access Control customers migrating to Access Controls 10x is that they want to take advantage of rule set changes made since their last rule set update, but they don't want to lose the customizations they've made to their existing rule set.

Additionally, business may also require a copy of the rule set for review by an external auditing firm or for backup purposes.

Ruleset can be transported, uploaded and downloaded from:

SPRO > IMG > GRC > AC > ARA > SOD Rules options.

Additionally, these tasks can be accomplished via two (2) Access Control transactions: "**GRAC_DOWNLOAD_RULES**" and "**GRAC_UPLOAD_RULES**".

Question # 37: Can we have different set of number ranges activated for request generation??

Number range is used to number the GRC Access requests. You may start your request numbers from 1 or xxxx01 or any other pattern that suits your business model.

To setup the number ranges, go to SPRO > IMG > GRC > Access Control > User Provisioning > Maintain Number Range Intervals for Provisioning Requests.

Here you can select **GRACREQNO** for all workflow requests created in GRC for access provisioning etc.

Then you can define the number range through Define Number Range for Provisioning Requests.

However, there can be only 1 number range that can be active.

Question # 38: What is a Workflow, Path and Stage?

Workflow: SAP GRC 10.0 introduced the new concept (well not so new now) of MSMP workflow engine as a configurable layer that sits on top of SAP Standard Workflow for Access Controls. This provides flexibility to enable a single request to be split and routed to different approvers in parallel as well as multiple approval steps depending on business requirements.

Path: Path is a group of stages with a start and end condition. For each Stage of a Path, an Approval Agent is specified (except for automatic approval where no agent is mentioned). The Manger Approval Agent will receive the request in their POWL inbox in GRC.

An additional Agent can be specified within task settings for escalation. If the Approval Agent for the stage does not respond in the specified time, the request will be routed to the escalated agent.

Stages: Every stage in the workflow will be associated with an action. Normally an Approval level.

Question # 39: What is an Agent? What are the different types of Agents?

Agent is the person who is directly/in-directly associated with the MSMP workflow. Agents are primarily classified in to 2 types:

- Approver Agent – A person who is defined in the MSMP stage with approval authorization is referred as approver agent. Approver agents can be:
    - Directly Mapped Users
    - PFCG User Group
    - PFCG Role
    - GRC API Roles
- Notification Agent – A person who will be notified upon a trigger point in every stage of the MSMP workflow. For eg: Approvers, Owners etc.,

Question # 40: Where from can we change the default expiration time for mitigating controls? What's the default value for the same?

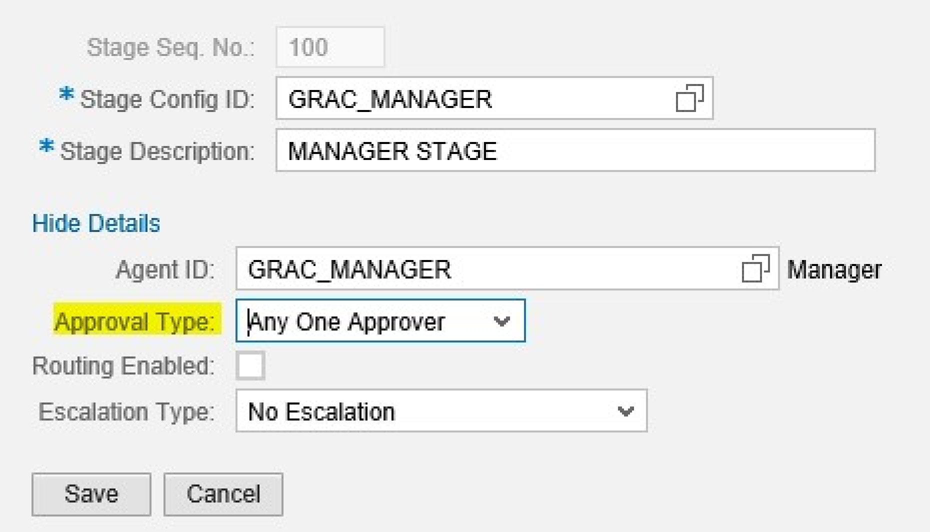
The default expiration for a mitigation control assignment can be changed with the parameter 1011 (Default expiration time for mitigating control assignments (in days)). By default the value is 365 days.

The default expiration for the users can be changed by performing the "SoD Review". Refer my video on configuring the various reviews @ www.youtube.com/sapsecurityexpert

Question # 41: What are the different types of Approval Types?

A request in a specific stage can be approved by either one user or all the users with similar authorization.

This can be defined using the Stage option – "Approval Type". Refer the screen below:



Stage Seq. No.: 100

* Stage Config ID: GRAC_MANAGER

* Stage Description: MANAGER STAGE

Hide Details

Agent ID: GRAC_MANAGER Manager

Approval Type: Any One Approver

Routing Enabled: □

Escalation Type: No Escalation

The default is "Any One Approver", in which the request goes to multiple approvers, but it can be approved by any of them.

When the "All Approvers" option is selected, the request in that STAGE should be approved by all the approvers.

Question # 42: How to modify the Notification Templates?

In GRC Access control as part of Workflow approvals and reviews Managers, Role Owners, FF ID Owners and Controllers, Function/Risk/Mitigation Approvers, Monitors, Users, Requestors etc. receive various Email notifications. Based on the client's requirements these Email notifications are enhanced and maintained. These templates can be modified by following the steps below:

1. Goto SE61 transaction code.
2. Select Document class as "General Text"
3. Copy the Document object ID from MSMP → 04 Variables & Templates
4. Enter the name and click Change.

The variables from the MSMP screen can be utilized in the notification templates. To know the detailed steps, check the following video:

https://www.youtube.com/watch?v=Ry85ARK_kXU

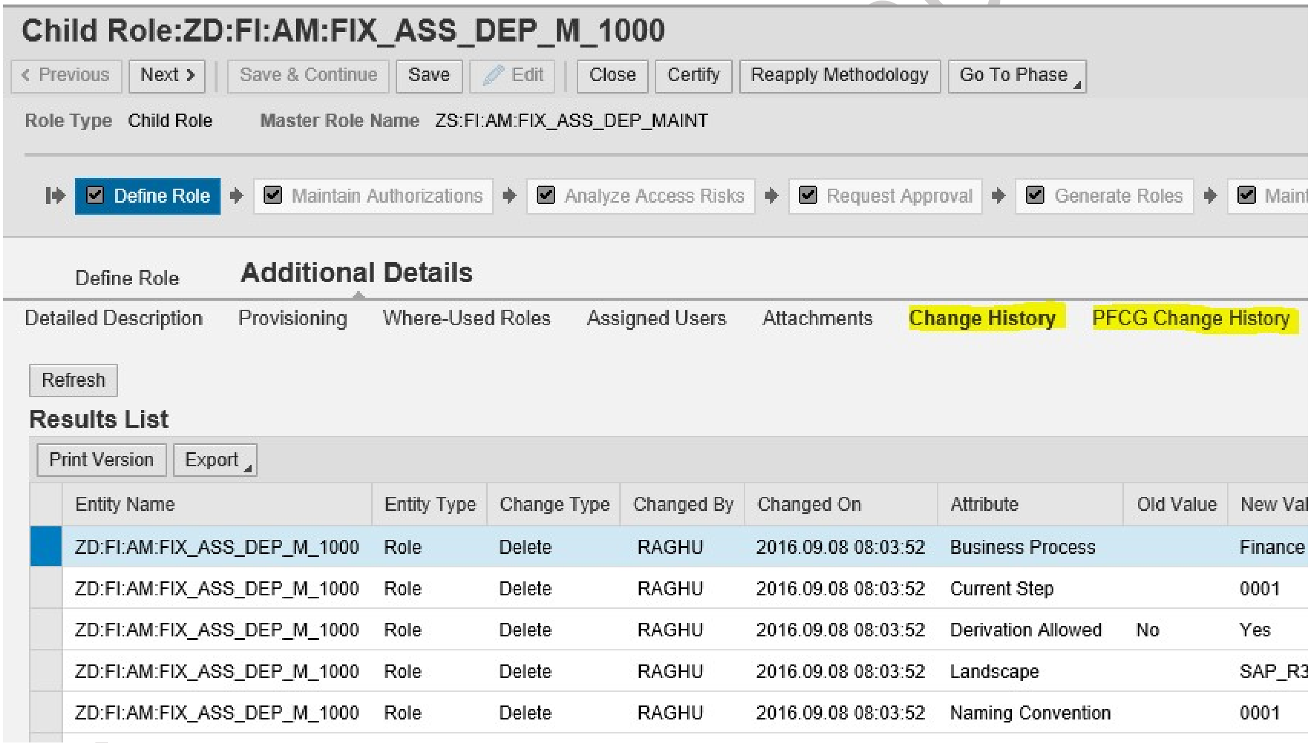
Question # 43: Can we view the changes of a role, happened in PFCG, through GRC?

The role creation process in BRM is tied to the PFCG, and controlled by the methodology setup. However, in GRC 10, change logs for role changes can be captured easily.

Setup the parameter - **1008** Enable Role Change Log

Further, changes logs can be viewed from the Role in the BRM repository. Simply open the role, and, goto Define Role > Additional Details

Change History – Shows the list of changes made from the BRM methodology
PFCG Change History – Changes made directly in the PFCG.



Child Role:ZD:FI:AM:FIX_ASS_DEP_M_1000

Role Type Child Role Master Role Name ZS:FI:AM:FIX_ASS_DEP_MAINT

Additional Details

Results List

Entity Name	Entity Type	Change Type	Changed By	Changed On	Attribute	Old Value	New Val
ZD:FI:AM:FIX_ASS_DEP_M_1000	Role	Delete	RAGHU	2016.09.08 08:03:52	Business Process		Finance
ZD:FI:AM:FIX_ASS_DEP_M_1000	Role	Delete	RAGHU	2016.09.08 08:03:52	Current Step		0001
ZD:FI:AM:FIX_ASS_DEP_M_1000	Role	Delete	RAGHU	2016.09.08 08:03:52	Derivation Allowed	No	Yes
ZD:FI:AM:FIX_ASS_DEP_M_1000	Role	Delete	RAGHU	2016.09.08 08:03:52	Landscape		SAP_R3
ZD:FI:AM:FIX_ASS_DEP_M_1000	Role	Delete	RAGHU	2016.09.08 08:03:52	Naming Convention		0001

Further, the differences can be easily identified using the Role mining options.

Question # 44: What is EUP? What is the default EUP ID?

In End user Personalization (simply called as EUP), user can set the parameters that define the behavior of the fields and the pushbuttons on the Request Access screen.

The default EUP template is 999. However, EUP templates can be created ranging from 001 to 998. To create/modify the EUP templates, use the follow path:

SPRO > IMG > GRC > AC > User Provisioning > Maintain End User Personalization

The below document explains the detailed steps to configure EUP:

https://wiki.scn.sap.com/wiki/display/GRC/End+User+Personalization+Configuration+Steps

Question#45: What is PSS (Password Self Service)? How to enable PSS for a specific connector?

Password Self Service is a customizing activity, which enables an end user to reset their own passwords in the back-end system. A user password is usually reset using TCode SU01. However considering this is restricted to end users and to help admins from being bogged down by constant password reset requests, a good alternative is to give the end user the option to reset their passwords themselves thereby freeing up the admins to do other tasks.

When an end user raises a request for a password reset, the application verifies the user based on the information they maintained for their password self-service settings or against the global PSS settings. Once the application verifies the user and the system, it resets the password and sends an e-mail to the user's configured e-mail address. The password sent is a generic password, which the user needs to change upon their login.

* All end users need to have a valid email ID to receive reset password link

For detailed steps to setup password self service, visit - http://scn.sap.com/docs/DOC-58058

Incase if the generated password is too long, you can define the length of the password too. Watch my video @ https://www.youtube.com/watch?v=etb71jkhN-A

Question # 46: What is the Purpose of EAM?

GRC AC Emergency Access Management (EAM) module, makes you Audit Ready by logging and tracking every activity that each user performs during an SAP Firefighting session.

It require users to provide detailed descriptions of their reasons for using the Firefighter ID along with their actions. This detailed documentation along with the transaction code execution report is automatically sent to the controller for a documented review.

Below are the quick points to remember about EAM:

- EAM allow users to take responsibility for task outside of their normal job function.
- Allow temporary access for users when assigned with solving problem, giving them provisionally broad, but regulated access.
- This temporary access will monitored and reviewed by the application.
- EAM provides the ability to manage and utilize firefighting activities centrally from the access control application
- The log files can be distributed to controller and owner via workflow for additional approval

Question # 47: What are the steps to create a new FFID and assign it to a Firefighter?

FFIDs are created as regular Dialog users only. Below steps detailed the complete process of creating and a FFID:

1. Create the FFID in the respective backend system as "SERVICE" type user.
2. Assign the relevant role(s) along with the role mentioned in the parameter 4010 (verify in both GRC & the backend system)
3. Run the "Repository Object" sync job in Incremental Mode in the GRC system (This will get the newly created FFID into the GRC repository)
4. Assign Owner (if admin does the controller assignment too, do that activity as well) from NWBC → Setup workcenter.
5. Ensure that the Owner & Controller has the EAM roles assigned in the GRC system.
6. Assign the FFID to Firefighters.

NOTE: Ensure that the authorizations assigned to the FFID are not available in the regular technical/business roles.

Question#48: In what cases a FFID is created?

You might have wondered why only few critical transaction codes access has moved to Firefighter, when there are 500+ critical transaction codes in SAP.

As a part of risk management, the priority is always given to risk remediation. If the risk can't be remediated, proper controls will be created and the risk will be mitigated. The criticality and the severity of the risk will be reduced during the mitigation process. Only the transaction codes for which the risks can't be either mitigated or remediated are transferred to the Firefighter application. All the relevant transactions are grouped and assigned to a Firefighter ID.

Question#49: Which all people are involved in EAM?

- Administrator – Can administer the complete application such as creating FF IDs, assigning FF IDs to the Owners, changing the parameter settings etc.,
- Owner – Can review the request and approve the FFID assignments, and has the authorization to assign Controllers, and FF IDs to Firefighter users.
- Controller – Will review the Notifications (Check in/out) and transaction execution logs.
- Firefighter – User who use a specific Firefighter ID.

Question#50: How can you assign the Firefighter ID?

Firefighter can be assigned in one of the following ways:

1. User can request for the Firefighter ID using the "Access Request" option by selecting the Firefighter ID or SPM user access. This will initiate the AR workflow and upon approval, user will get access to the Firefighter ID.
2. From NWBC → Setup Work centre, Admin/Owner can assign the Firefighter ID to the Firefighter. (This is the manual process).

References & Acknowledgements:

- These FAQs are compiled from various sources and also with the experience of the author.
- Some part of the answers were extracted from SCN Documents, Wispubs, SAP Help and other sources.
- Thanks for everyone author/expert who are directly or in-directly involved in preparing this FAQs publication.